1.1.1 "DEBUG" Modunun Açık Olması (Debug Mode Enabled) (CWE-11)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Uygulama geliştirme sırasında geliştiriciler genellikle testing (test etme) ve debugging (hata ayıklama) faaliyetlerini kolaylaştırmak için özelleştirilmiş kodlamalarda bulunurlar. Bu testing ve debugging (hata ayıklama) kodları prod ortama deploy edilirlerse (dağıtılırlarsa) bazu güvenlik riskleri ortaya çıkarırlar. Bu ortaya çıkabilecek risklere örnek olarak şunlar verilebilir:

- Uygulamada sunulanın dışında girdi noktaları oluşabilir. Bu ise uygulamanın saldırı yüzeyini arttırdığından uygulamanın güvenlik seviyesini düşürücü etkiye sahiptir.
- Bu türden kodlar normal uygulama kodları gibi düzgün bir şekilde test edilmediklerinden ve bakımı yapılmadıklarından uygulama kodlarının diğer bölümlerinde düzeltilen artık geçmişte kalmış açıklıkların varlığını sunabilirler.
- Bu türden kodlar sıklıkla geliştiricinin testlerini kolaylaştırmak amacıyla geliştiricinin güvenlik mekanizmalarını (örn; kimlik doğrulama veya erişim kontrollerini) bypass'layabileceği (atlatabileceği) ve doğrudan hata ayıklaması yapacağı fonksiyonelliğe ulaşabileceği backdoor'lara (arka kapılara) sahip olabilirler.

Eğer bir uygulamanın prod ortamında debug (hata ayıklama) modu açıksa tüm bu olası riskler saldırganların yapacağı saldırıları kolaylaştırıcı etkiye sahiptir. Bu riskler saldırganlara uygulamayı öğrenme noktasında, ayrıca framework'e, veritabanına ve diğer kaynaklara karşı saldırı çeşitleri planlama noktasında yardımcı olur. Bu modun açık olduğu uygulamalarda "Debug Modunun Açık Olması (CWE-11)" açıklığı vardır denir.

Kurum uygulamada debug modun açık olduğu tespit edilmiştir:

:::::BULGU:::::

Açıklığın Önlemi:

Sorun gidermek isteyen geliştiriciler debug modu ile uygulamalarının çalışma akışını daha yakından kontrol ederler ve gözlemlerler. Fakat bu mod prod ortamda kapalı tutulmalıdır. Açıklığın kapatılması için gerekli öneriler şu şekildedir:

- Uygulamayı derlemeden önce veya deploy etmeden önce tüm debugging (hata ayıklama) kodlarını silin.
- Yapılandırma ayarlarından debug modunun açık olmadığından emin olun.
- Tüm test kodlarını uygulamanın geri kalan kodlarından izole olan ve test amaçlı var olan test framework'lerinde uygulayın.
- Uygulama kaynak kodlarının kendisinde özel test kodları, debugging (hata ayıklama) kodları ve gizli geliştirici arayüzleri ile gizli geliştirici parametreleri kullanmaktan kaçının.
- Otomatik olarak deploy edilmiş uygulamayı konfigure edebilecek, tüm geçici kodları dışlayabilecek ve sadece asıl uygulama kodlarını dahil edecek standart ve otomatik bir build / deployment süreci tanımlayın ve uygulayın.

Java uygulamalarda debug modunun açık olduğunu gösterir kod bloğu örneği paylaşılmıştır:

Java:

```
// GÜVENSİZ KOD

public class AppServlet extends HttpServlet {
      protected void doGet(HttpServletRequest request, HttpServletResponse
response)
                              throws ServletException, IOException {

            // Talebi uygula.
    }

      private static String MODE = "";

      public static void main(String[] args) {

            // Uygulamayı test ve debugging için ayarla.
            MODE = "DEBUGGING";
    }
}
```

Ruby uygulamalarda debug modunun açık olduğunu gösterir kod bloğu örneği paylaşılmıştır:

Ruby:

```ruby
# GÜVENSİZ KOD BLOĞU

class AppClass

      def run_app

          # Uygulamayı çalıştır.

      end

      def test_app

            # Uygulamayı test ve debug eden kodlar bölümü.

      End

end
```

.NET uygulamalarda debug modunu kapamak için web.config yapılandırma dosyasında <system.web> … </system.web> etiketleri arasında yer alan <compilation etiketinin debug özelliği true yerine false yapılmalıdır.

```xml
<!-- GÜVENSİZ YAPILANDIRMA -->

<?xml version="1.0" encoding="utf-8"?>
<configuration>
   ...
   <system.web>
      <compilation debug="true" ...>
      ...
   </system.web>
   ...
</configuration>
```

```
<!-- GÜVENLİ YAPILANDIRMA -->

<?xml version="1.0" encoding="utf-8"?>
<configuration>
   ...
   <system.web>
      <compilation debug="false" ...>
      ...
   </system.web>
   ...
</configuration>
```

Bu yapılandırma ayarında yapılan sıkılaştırma ile "DEBUG" modu production (yayın) ortamı için kapatılmış olur ve herhangi bir hata ya da olağandışı durumda uygulamaya ait bilgi dökümü istemci taraftan görülmez.

Referanslar:

1. https://docs.microsoft.com/en-us/troubleshoot/aspnet/disable-debugging-application
2. https://cwe.mitre.org/data/definitions/11.html
3. https://gist.github.com/marcbarry/47644b4a43fbfb63ef54